INSTRUCTIONS

Version 1.0

"C-SCRM QUESTIONNAIRE" EXCEL WORKSHEET COMPLETION INSTRUCTIONS:

- This worksheet shall be completed by the vendor responsible for submitting the offer. References to "organization" refer to the offering entity. If the offering entity is a joint venture (JV), the response may come from either the JV or from the JV managing partner.
- Provide the requested inputs in the gray shaded lines of the template under column D, Vendor Response, for all Items Numbers for Sections 1-3. Offerors are advised that the Government may request documentation from the Offerors to validate the responses provided.

"SOFTWARE PRODUCER ATTESTATION" EXCEL WORKSHEET COMPLETION INSTRUCTIONS:

- NIST White Paper "Definition of Critical Software Under Executive Order (EO) 14028" dated October 13, 2021 defines critical software. Complete this worksheet by providing the requested inputs in the gray shaded lines of the template under columns C-D if your firm or your subcontractors are offering to supply critical software to the Government as part of your firm's offer. This worksheet must be completed by each software producer that will be supplying critical software as part of your firm's offer. If critical software is not being provided by your firm or subcontractors, please enter N/A in said gray shaded lines of the template.

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) SOFTWARE PRODUCER ATTESTATION FORM

This form must be completed by the software producer.

ITEM NUMBER	ITEM DESCRIPTION	VENDOR RESPONSE
1.1	Enter the name of the software producer.	
1.2	Provide a statement attesting that the software products listed in Item Number 1.3 of this form follow the secure development "practices" and "tasks" identified in NIST SP 800-218. A summary of these practices and tasks are provided below for reference from NIST SP 800-218. If you cannot attest to all practices and tasks, identify the ones that you attest to and the ones that you cannot attest to. For those practices and tasks that you cannot attest to, describe the practices that you have in place to mitigate those risks (i.e., risks for practices or tasks you cannon attest to), and provide a Plan of Action & Milestones (POA&M) detailing how your firm will reach compliance for those non-compliant practices and tasks.	
1.3	A description of which product or products the statement provided for Item Number 1.2 refers to (preferably focused at the company or product line level and inclusive of all unclassified products sold to Federal agencies).	

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) QUESTIONNAIRE

SECTION 1 - CONTACT INFORMATION

ITEM NO.	ITEM DESCRIPTION	VENDOR RESPONSE	
1.1	Enter the name of your company.		
1.2	Enter the name of the primary Point-Of-Contact (POC) for your company that the Government may contact to discuss the vendor inputs on this questionnaire.		
1.3	Enter the job title of the primary POC.		
1.4	Enter the phone number of the primary POC in the following format: (555) 555-5555		
1.5	Enter the e-mail address of the primary POC.		

SECTION 2 VENDOR RISK MANAGEMENT PLAN

ITEM NO.	ITEM DESCRIPTION	VENDOR RESPONSE	NIST SP 800-53 Reference
2.1	Does your organization identify its key supply chain threats?		IR-8, SR-7
2.2	Does your organization map key suppliers to your supply chain threats?		IR-8, SR-7
2.3	Do you have a policy or process to ensure that none of your suppliers or third-party components have an active exclusion record in the System for Award Management (https://sam.gov)?		SAM.gov
2.4	Does your organization have written SCRM requirements in contracts with your key suppliers?		SA-4
2.5	Does your organization verify that your suppliers meet SCRM requirements through contractual terms and conditions?		SR-6

SECTION 3 PHYSICAL AND PERSONNEL SECURITY

ITEM NO.	ITEM DESCRIPTION	VENDOR RESPONSE	NIST SP 800-53 Reference
3.1	Does your organization have policies for conducting background checks of your employees as permitted by the country in which your organization operates?		PE-2, PE-3 PS-3
3.2	Does your organization have procedures in place to prevent tampering of Information and Communications Technology (ICT) equipment stored as supply chain inventory?		SR-9 AC-1
3.3	Do you provide literacy training on recognizing and reporting potential indicators of insider threat?		AT-2(2)